



## How good are some 2nd round SHA3 hashes when their compression functions are weak?

Gauravaram, Praveen

*Publication date:*  
2010

*Document Version*  
Publisher's PDF, also known as Version of record

[Link back to DTU Orbit](#)

*Citation (APA):*  
Gauravaram, P. (Author). (2010). How good are some 2nd round SHA3 hashes when their compression functions are weak?. Sound/Visual production (digital) <http://rump2010.cr.yp.to/>

---

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# How good are some 2<sup>nd</sup> round SHA3 hashes when their compression functions are weak? (Work in progress)

Charles Bouillaguet, Pierre-Alain Fouque, Praveen Gauravaram\*  
and Gaëtan Leurent

ENS, France and DTU, Denmark\*

17th August 2010

It is a folklore that some attacks on compression functions do not weaken hash functions.

It is a folklore that some attacks on compression functions do not weaken hash functions.

When can we say that even after doing some strong attack on the compression function, the above belief on the hash function security would still hold?

# On some SHA3 hash functions

- ① Nearly all SHA3 designers who have had distinguishers, symmetries, fixed points, partial fixed point etc.. sort of analysis on their compression functions claimed that they do not lead to attacks on hash functions.
- ② Some designers (e.g SIMD, SHABAL) even proved the indistinguishability security of their hash function when the compression function has efficient distinguishers.

Are these hash functions still indifferentiable if their compression functions are easily invertible (pseudo preimage attacks)?

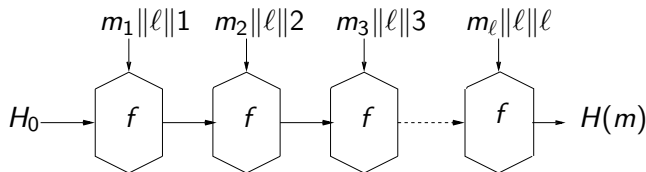
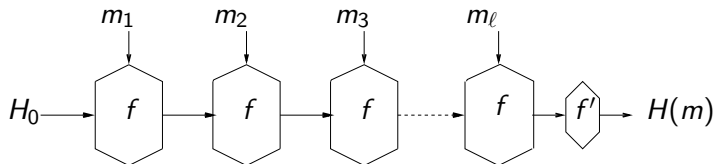
# On some SHA3 hash functions

- ① Nearly all SHA3 designers who have had distinguishers, symmetries, fixed points, partial fixed point etc.. sort of analysis on their compression functions claimed that they do not lead to attacks on hash functions.
- ② Some designers (e.g SIMD, SHABAL) even proved the indistinguishability security of their hash function when the compression function has efficient distinguishers.

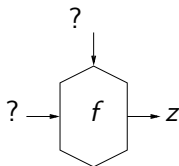
Are these hash functions still indifferentiable if their compression functions are easily invertible (pseudo preimage attacks)?

Many second round SHA3 hash functions use a wide-pipe or a pfMD or their special instantiation for the iteration.

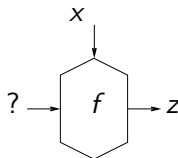
# Wide-pipe and pfMD



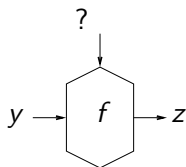
# Invertible queries to compression functions



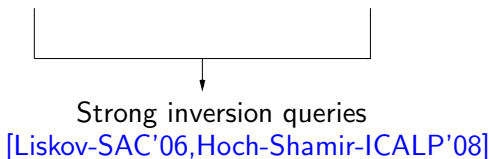
Weak backward query  
[We consider]



Strong backward query



Bridging query





# Indifferentiability results

| Mode            | pfMD | wide pipe          |
|-----------------|------|--------------------|
| Bridging        | no   | no                 |
| Strong backward | no   | yes* [SHABAL team] |
| Weak backward   | yes  | yes* [SHABAL team] |

- 1 Generalisation of indifferentiability of Sponge hash construction[Bertoni *et al.*-Eurocrypt'08].
- 2 Wide-pipe of a weak compression function such as Rabin's 78 scheme seems to remain indifferentiable [SHABAL team].

Thank you!!!!